Приложение № 1
к приказу министерства здравоохранения
Нижегородской области

от "___" _____ 2020 г. №_____

ПОЛИТИКА

по вопросам обработки и обеспечения защиты информации, содержащей персональные данные в региональном сегменте единой информационной системы в сфере здравоохранения Нижегородской области

Нижний Новгород
2020

СОДЕРЖАНИЕ

1. Общие положения

Настоящая Политика по вопросам обработки и обеспечения защиты информации (далее – Политика), содержащей персональные данные (далее – ПДн), в Региональном сегменте единой информационной системы (РС ЕИСЗ) в сфере здравоохранения Нижегородской области (далее – МИС) является официальным документом министерства здравоохранения Нижегородской области (далее - Министерство).

МИС создана в рамках программы модернизации здравоохранения Нижегородской области в 2011-2012 годах. Разработка МИС выполнена на основании системного проекта «Создание регионального сегмента единой информационной системы в сфере здравоохранения Нижегородской области, с поддержкой процесса управления оказания медицинской помощи населению и повышения информированности населения» (далее – Системный проект), утвержденного министром здравоохранения Нижегородской области.

Обеспечение безопасности ПДн является одной из приоритетных задач функционирования МИС. Целью разработки настоящей Политики являются определение принципов и особенностей обработки и обеспечения безопасности ПДн, обрабатываемых в МИС.

Политика разработана в соответствии с требованиями действующего законодательства РФ по вопросам обработки и защиты ПДн.

В Политике отражается система взглядов Министерства, как Оператора по обработке ПДн в МИС, относительно вопросов обеспечения безопасности ПДн в МИС.

Настоящая Политика определяет принципы, порядок и условия обработки ПДн в МИС с целью обеспечения защиты прав и свобод человека и гражданина при обработке его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также устанавливает ответственность должностных лиц, имеющих доступ к ПДн, за невыполнение требований норм, регулирующих обработку и защиту ПДн.

Положения Политики распространяются на Министерство, а также все подведомственные ему организации и обязательны к исполнению всеми сотрудниками Министерства и государственных бюджетных учреждений здравоохранения Нижегородской области (далее - ГБУЗ НО) (штатных, временных, работающих по контракту и т.п.), допущенных к обработке ПДн в МИС, а также всем лицам, имеющим доступ к ресурсам МИС, в том числе сотрудников сторонних организаций, оказывающих услуги по обслуживанию программных и технических средств МИС (подрядчики, аудиторы и т.п.).

Настоящая Политика является публичным документом неограниченного доступа, реализуемого путем публикации в открытом источнике или иным образом в соответствии с п. 2 ст. 18.1 Федерального закона «О персональных данных».

1.1 Порядок ввода в действие, внесения изменений и ознакомления с Политикой.

Политика утверждается и вводится в действие приказом Министерства.

Изменения в Политику вносятся приказом Министерства.

Работники Министерства, а также ГБУЗ НО, имеющие доступ к обработке ПДн в МИС, должны быть ознакомлены с Политикой под роспись. При заключении договоров со сторонними организациями, оказывающими услуги по обслуживанию программных и технических средств МИС, обязательно должно быть заключено Соглашение о конфиденциальности, содержащее положения Политики, с которым сотрудники подрядной организации должны быть ознакомлены под роспись.

2. Обработка ПДн в МИС

2.1 . Структура МИС

МИС Нижегородской области состоит из центрального сегмента – центра обработки данных (ЦОД), а также территориально удаленных сегментов, располагающихся в ГБУЗ НО:

- Информационная система персональных данных (далее – ИСПДн) «МИС. Сегмент ЦОД» (1 шт.) Оператор ИС – государственное бюджетное учреждение здравоохранения Нижегородской области «Медицинский информационно-аналитический центр» (далее - ГБУЗ НО МИАЦ);
- ИСПДн «МИС. Сегмент ГБУЗ НО» (144 шт.) Операторы ИС – ГБУЗ НО.

Перечень ИСПДн МИС утверждается министром здравоохранения Нижегородской области.

Основные вычислительные мощности МИС по обработке и хранению информации представлены в ИСПДн «МИС. Сегмент ЦОД».

ИСПДн «МИС. Сегмент ГБУЗ НО» фактически представляет собой набор рабочих мест пользователей прикладного комплекса МИС, объединенных выделенным сегментом локальной вычислительной сети в пределах одного ГБУЗ НО, и подключенных к выделенным каналам связи для связи с ЦОД.

2.2. Состав ПДн

Перечень ПДн, обрабатываемых в МИС и подлежащих защите, формируется в соответствии с Федеральным законом России от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и Системным Проектом.

Полный состав ПДн, обрабатываемых в МИС, утверждается Министром здравоохранения Нижегородской области.

В МИС обрабатываются ПДн, содержащие информацию о состоянии здоровья граждан, относящуюся к специальным категориям ПДн.

2.3. Виды обработки ПДн

В МИС производится обработка ПДн с использованием средств автоматизации (автоматизированная обработка), включая: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение),

извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

2.4. **Принципы обработки ПДн**

Обработка ПДн в МИС должна осуществляться на законной и справедливой основе в соответствии с принципами, определенными в Статье 5 ФЗ РФ от 27 июля 2006 г. № 152-ФЗ «О Персональных данных».

2.5. **Правовые основания обработки ПДн**

Обработка ПДн осуществляется на основании:

- Конституции Российской Федерации;
- Федерального закона Российской Федерации от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федерального закона от 29.11.2010 № 326-ФЗ «Об обязательном Медицинском страховании в Российской Федерации»;
- Федерального закона от 17.07.1999 № 178-ФЗ «О государственной социальной помощи»;
- Федерального закона от 16.07.1999 № 165-ФЗ «Об основах обязательного социального страхования»;
- Положения о министерстве здравоохранения Нижегородской области, утвержденного Постановлением Правительства Нижегородской области от 23 ноября 2007 г. № 435 (в ред. постановлений Правительства Нижегородской области от 20.06.2008 № 245, от 07.08.2008 № 330, от 19.11.2008 № 550);
- обязанностей по предоставлению государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», для обеспечения предоставления такой услуги;
- согласия субъекта ПДн на обработку его ПДн;
- необходимости обработки ПДн для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или

договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;

- в случаях, когда обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно.

2.6. **Цели обработки ПДн**

Исполнение государственных функций, отнесенных к компетенции министерства здравоохранения Нижегородской области и закрепленных в положении о министерстве здравоохранения Нижегородской области.

2.7. **Обработка ПДн**

Заказчиком МИС и оператором, организующим обработку информации, содержащую ПДн (далее - Оператор ПДн) в МИС является Министерство здравоохранения Нижегородской области.

Министерство здравоохранения НО, как оператор ПДн МИС, определяет цели обработки ПДн, сроки, требования по обработке и обеспечению безопасности безопасности ПДн.

В соответствии с положениями Федерального закона «О ПДн» ответственность перед субъектами ПДн (гражданами) и контролирующими органами несет Оператор ПДн. Лица, обрабатывающие ПДн по поручению Оператора несут ответственность перед Оператором.

2.7.1. Операторы информационных систем

Операторами информационных систем, в соответствии с положениями Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ, назначены и являются:

- ИСПДн «МИС. Сегмент ЦОД» - ГБУЗ МИАЦ НО;
- ИСПДн «МИС. Сегмент ГБУЗ» - ГБУЗ НО соответствующего муниципального образования Нижегородской области.

2.7.2. Поручение обработки ПДн

В соответствии с п.3 ст.6 Федерального закона «О ПДн» Министерство здравоохранения НО поручает каждому Учреждению здравоохранения

Нижегородской области проводить обработку ПДн в информационной системе ПДн – сегменте МИС Нижегородской области, оператором которой является данное Учреждение здравоохранение.

2.7.3. Ответственные лица

Приказом Министра здравоохранения назначается лицо, ответственное за обработку ПДн в МИС, а также создается комиссия по вопросам обработки ПДн в МИС.

Обработка ПДн:

Ответственные лица за организацию обработки ПДн:

- ИСПДн «МИС. Сегмент ЦОД» - руководитель ГБУЗ МИАЦ НО;
- ИСПДн «МИС. Сегмент ГБУЗ» - руководитель ГБУЗ НО соответствующего муниципального образования Нижегородской области.

Организация защиты ПДн:

Подразделение, ответственное за организацию и обеспечение защиты ПДн в МИС - ГБУЗ НО «МИАЦ НО».

Обеспечение защиты ПДн:

- ИСПДн «МИС. Сегмент ЦОД» - сотрудники ГБУЗ МИАЦ НО, исполняющие функции администратора системы и администратора информационной безопасности;
- ИСПДн «МИС. Сегмент ГБУЗ» - сотрудник(и) ГБУЗ НО соответствующего муниципального образования Нижегородской области, исполняющий(ие) функции администратора системы и администратора информационной безопасности сегмента МИС.

2.7.4. Сроки обработки ПДн

Сроки обработки ПДн в МИС не должны превышать сроки, определенные законодательством РФ об охране здоровья граждан.

2.7.5. Права и обязанности Оператора ПДн

Оператор ПДн МИС вправе:

- организовывать и проводить обработку ПДн в составе и объеме, соответствующим определенным и законным целям;

- использовать ПДн Субъекта ПДн без его согласия, в случаях предусмотренных законодательством.
- уточнять и получать дополнительные ПДн у Субъекта ПДн и(или) у его законных представителей, необходимые для целей обработки ПДн в МИС;
- поручить обработку ПДн третьим другому лицу с согласия Субъекта ПДн либо без такового в случаях, предусмотренных ФЗ РФ от 27 июля 2006 г. № 152-ФЗ «О ПДн».
- предоставлять ПДн субъектов ПДн третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);
- отказывать в предоставлении ПДн в случаях предусмотренных законодательством.

Оператор ПДн обязан:

- Осуществлять обработку ПДн с соблюдением принципов и правил, предусмотренных ФЗ РФ от 27 июля 2006 г. № 152-ФЗ «О ПДн».
- Соблюдать требования действующего законодательства по вопросам обработки и защиты ПДн;
- Обеспечивать точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Принимать меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;
- Хранить ПДн в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн.
- Уведомить уполномоченный орган по защите прав субъектов ПДн об обработке ПДн в МИС в соответствии с положениями ФЗ РФ от 27 июля 2006 г. № 152-ФЗ «О ПДн».

2.7.6. Права и обязанности субъекта ПДн

Субъект ПДн имеет право на получение сведений, касающихся обработки его ПДн в МИС, требовать от оператора уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими,

неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Если субъект ПДн считает, что оператор осуществляет обработку его ПДн с нарушением требований настоящего Федерального закона или иным образом нарушает его права и свободы, субъект ПДн вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке.

Субъект ПДн имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Реализация указанных прав субъектов ПДн осуществляется в соответствии с положениями Федерального закона «О ПДн».

2.8. **Ответственность за нарушение требований по обеспечению безопасности ПДн**

В соответствии со ст. 24 Федерального закона «О ПДн» лица, виновные в нарушении требований данного Федерального закона, несут предусмотренную законодательством РФ ответственность.

3. Система защиты ПДн

Безопасность ПДн, обрабатываемых в МИС, обеспечивается системой защиты ПДн МИС – СЗПДн МИС, включающей проведение организационных и технических мероприятий по обеспечению безопасности ПДн.

СЗПДн МИС реализована в соответствии с требованиями действующего законодательства по защите ПДн, Системного проекта, а также разработанных моделей угроз безопасности ПДн и моделей нарушителей, актов классификации ИСПДн.

Цель создания СЗПДн - минимизация ущерба, который может возникнуть вследствие воздействия угроз информационной безопасности, приводящих к нарушению требуемых свойств безопасности ПДн, обрабатываемых в МИС Нижегородской области.

3.2. Организационные мероприятия

- Назначены ответственные лица за организацию обработки информации, содержащей ПДн в МИС Нижегородской области, а также за организацию и обеспечение безопасности ПДн при их обработке в МИС;
- Определены принципы и условия обработки ПДн в МИС;
- Определен перечень ПДн, обрабатываемых в МИС и подлежащих защите;
- Определен список ИСПДн, взаимодействующих с МИС, условия их функционирования;
- Проведена классификация ИСПДн;
- Разработаны модели угроз безопасности ПДн и модели нарушителя, проектные документы по созданию СЗПДн МИС;
- Разработан пакет организационно-правовых документов (ОРД) Министерства здравоохранения Нижегородской области по вопросам обработки и защиты ПДн в МИС, включающий:
- Настоящую Политику информационной безопасности;
- Положение по обеспечению безопасности ПДн при их обработке в информационных системах ПДн в МИС;
- Регламенты, инструкции, журналы;

- Утвержден список лиц, допущенных к работе в МИС, определены их роли и регламент доступа к ресурсам ИСПДн;
- Положения ОРД доведены до сотрудников под роспись;
- Определен план мероприятий по обеспечению защиты ПДн.

3.3. **Технические мероприятия**

- Обеспечен режим физической охраны средств вычислительной техники МИС;
- Реализовано проектное решение по создании, СЗПДн, нейтрализующее актуальные угрозы безопасности с использованием сертифицированных средств защиты информации.

3.4. **Аттестация**

Для подтверждения соответствия ИСПДн МИС требованиям действующего законодательства проводятся аттестационные испытания систем.

Повторная аттестация государственной информационной системы осуществляется в случае окончания срока действия аттестата соответствия или повышения класса защищенности информационной системы. При увеличении состава угроз безопасности информации или изменения проектных решений, реализованных при создании системы защиты информации информационной системы, проводятся дополнительные аттестационные испытания в рамках действующего аттестата соответствия.

Ввод в действие и эксплуатация информационной системы производится только при наличии аттестата соответствия.

4. Заключительные положения

Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите ПДн.

Контроль исполнения требований настоящей Политики осуществляется лицом, ответственным за обеспечение безопасности ПДн в МИС.

5. Законодательная, нормативная и методическая база

Федерального закона от 27 июля 2006 г. № 152-ФЗ «О ПДн», а также следующих документов:

Данный документ учитывает требования следующих законодательных актов и нормативно-методических документов:

- Требования к защите ПДн при их обработке в информационных системах ПДн, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119;
- Постановление Правительства Российской Федерации от 21 марта 2012 г. N 211 г. Москва "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О ПДн" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами";
- Требования по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. N 17;
- Состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн», утвержденные приказом ФСТЭК России от «18» февраля 2013 г. N 21;
- «Базовая модель угроз безопасности ПДн при их обработке в ИСПДн», утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.;
- «Методика определения актуальных угроз безопасности ПДн при их обработке в ИСПДн», утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г;
- «Методические рекомендации по обеспечению с помощью криптосредств безопасности ПДн при их обработке в информационных системах ПДн с использованием средств автоматизации» утвержденные руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/5-144;
- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты

информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности ПДн при их обработке в информационных системах ПДн», утвержденные руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/6/6-622;

- ГОСТ РО 0043-003-2012 , ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний»;
- Информационное сообщение по вопросам защиты информации и обеспечения безопасности ПДн при их обработке в информационных системах в связи с изданием приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн» от 15 июля 2013 г. № 240/22/2637.
- «Требованиями к защите ПДн при их обработке в информационных системах ПДн», утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119;
- «Положение о методах и способах защиты информации в информационных системах ПДн», утвержденное приказом ФСТЭК России 05 февраля 2010 г. № 58;
- «Методические рекомендации по обеспечению с помощью криптосредств безопасности ПДн при их обработке в информационных системах ПДн с использованием средств автоматизации» утвержденные руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/5-144;
- «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае из использования для обеспечения безопасности ПДн при их обработке в

информационных системах ПДн», утвержденных руководством 8 Центра ФСБ России 21.02.2008 г. № 149/6/6-662;

- Системного проекта «Создание регионального сегмента единой информационной системы в сфере здравоохранения Нижегородской области, с поддержкой процесса управления оказания медицинской помощи населению и повышения информированности населения», разработанный в рамках реализации программы модернизации здравоохранения Нижегородской области (далее – Системный проект).